Piratage de Free : des cybercriminels prétendaient avoir vendu les données de 19 millions d'utilisateurs dont l'IBAN de 5 millions d'entre eux.

Et si les données n'avaient pas été vendues ?

Le 7 novembre 2024 à 00:41, par Stéphane le calme | **0 commentaire**

0 PARTAGES | 4 | 0

Fin octobre, Free a été victime d'un piratage historique. Des cybercriminels ont ciblé l'un des outils de gestion de l'opérateur et sont parvenus à récupérer les données personnelles de plus de 19 millions de clients Free Mobile et Freebox. Il s'agit notamment du nom/prénom, de l'adresse mail et postale, de la date et lieu de naissance, du numéro de téléphone ou encore de l'identifiant abonné et des données contractuelles. Ils se sont également emparés des IBAN de plus de 5 millions de clients. Comme le veut la loi dans ce genre d'affaire, Free a rapidement notifié l'attaque auprès de la CNIL et de l'ANSSI. Un formulaire en ligne était censé être mis en place la semaine dernière, pour faciliter le dépôt de plainte des très nombreuses victimes de la cyberattaque de Free. Mais le projet a finalement été abandonné.

Le 22 octobre, un utilisateur d'un forum bien connu des cybercriminels, annonçait disposer de données personnelles de millions de clients de l'opérateur Free. Il disait chercher à les vendre au plus offrant.

Le vol de données a été confirmé quelques jours plus tard par Free. Le fournisseur d'accès à Internet a confirmé qu'il avait été piraté après qu'un cybercriminel se faisant appeler « drussellx » a mis aux enchères les données de ses clients sur ledit forum.

Les noms, prénoms, adresses e-mail et postale, dates et lieux de naissance, numéros de téléphone, identifiants abonné et données contractuelles de dizaines de milliers de clients ont ainsi été dérobés, comme l'indiquait Free dans un e-mail transmis à ses souscripteurs concernés.

Seulement, selon l'ingénieur en cybersécurité Clément Domingo, les IBAN (pour « International Bank Account Number »), code qui permet d'identifier un compte en banque, ont également été dérobés lors de cette attaque.

> La nuit dernière à 4h30 du matin, le cybercriminel à l'origine de la cyberattaque de Free à diffusé un échantillon de 100 000 IBAN sur les 5,11M qu'il dit détenir.
>
> Cette nouvelle publication est certainement en réaction avec le mail de Free, probablement qu'il a trouvé laxiste... et qui ne mentionnait guère la compromission des IBAN...
>
> Son message est de plus sans équivoque avec une photo reprenant le titre du dernier livre de Xavier Niel, "Une sacrée envie de foutre le bordel" ! Faut croire que ce cybercriminel est entrain de le faire...

🚨🔴CYBERALERT, 🇫🇷FRANCE 🔴 | Cyberattaque Free, 100 000 IBAN diffusés gratuitement sur le "Amazon de la cybercriminalité" par le même cybercriminel français

La nuit dernière à 4h30 du matin, le cybercriminel à l'origine de la cyberattaque de Free à diffusé un échantillon de 100… pic.twitter.com/qPzE0Yq5bn

— SaxX ¯_(ツ)_/¯ (@_SaxX_) October 27, 2024

Le vol de ces IBAN a été confirmé par Free, dimanche, dans un courriel envoyé à certains de ses clients.

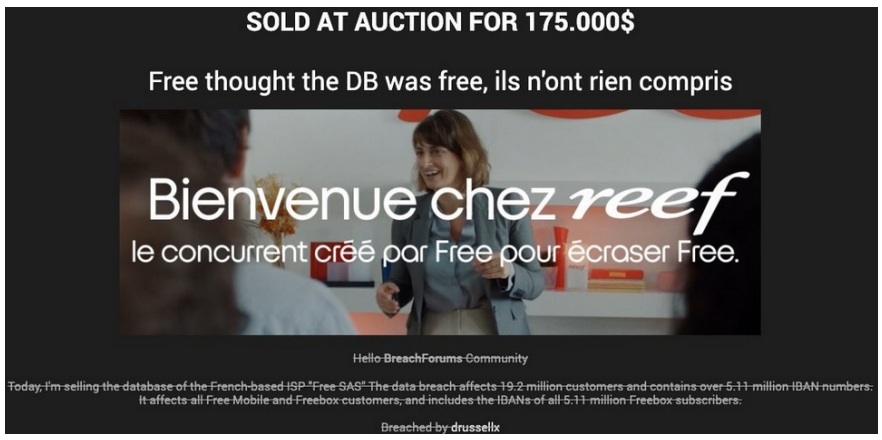
Drussellx a affirmé avoir acquis les informations de 19,2 millions d'abonnés, dont cinq millions accompagnés des IBAN (pour des abonnés Freebox uniquement), le 17 octobre 2024. La violation « affecte tous les clients FREE Mobile et Freebox, et comprend les IBAN des 5,11 millions d'abonnés Freebox », a écrit drussellx.

En reconnaissant la faille, FREE a indiqué que l'attaquant avait ciblé un outil de gestion qui lui permettait d'accéder aux données des abonnés, mais pas aux mots de passe, aux informations des cartes bancaires ou au contenu des communications. La société, qui est une filiale du groupe Iliad, a ensuite déposé une plainte pénale et a notifié l'incident à la CNIL et à l'ANSSI.

L'un des cybercriminels affirme avoir vendu les données

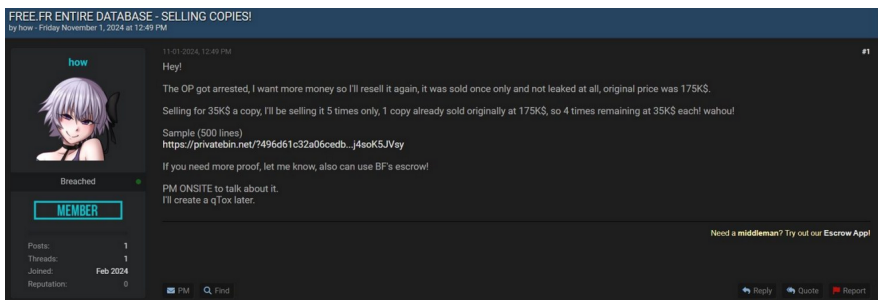
Durant le week-end, drussellx a indiqué mettre aux enchères un fichier contenant pas moins de 100 000 lignes, avec des données personnelles de clients, dont les IBAN correspondants évidemment : « Si l'entreprise ne participe pas à cette unique vente aux enchères dans les prochains jours, cette copie sera vendue, ce qui entraînera de graves conséquences pour les clients, et sera probablement divulguée publiquement sur les forums dans un avenir proche », affirmait-il.

Quelques jours plus tard, un autre message est apparu. Celui-ci affirmait que les données avaient été vendues aux enchères pour 175 000 dollars. « Free thought the DB was free, ils n'ont rien compris », pouvait-on lire.



Mais l'annonce de la vente n'annonçait pas la fin de l'histoire, semble-t-il.

Le 1er novembre, un autre utilisateur du forum se faisant appeler « how » a posté que l'auteur du post original avait été arrêté et qu'il revendait les données pour gagner plus d'argent à 35 000 dollars par copie, cinq fois seulement. Il a fourni le même échantillon de données que dans le message original et a invité les gens à lui envoyer des messages privés. DataBreaches l'a contacté par message privé pour lui poser des questions parce que le message ressemblait à une arnaque. Il n'a jamais répondu à DataBreaches mais a retiré son message.



Et si les données personnelles et bancaires des clients de Free récupérées par un pirate n'avaient finalement pas été vendues ?

Le 3 novembre, l'histoire a pris une tournure surprenante. DataBreaches a été contacté par quelqu'un qui s'est identifié comme « YuroSh ». Il a affirmé être le pirate responsable de la fuite sur free.fr. « Je comprends que cette base de données a été présentée à la télévision française pendant des semaines, et j'aimerais clarifier quelques détails », a-t-il déclaré, fournissant à DataBreaches ce qui semble être les informations personnelles de Xavier Niel (PDG de FREE) comme preuve préliminaire de son implication.

Interrogé, YuroSh a déclaré que son rôle avait été d'aider à exploiter la vulnérabilité. DataBreaches lui a demandé de demander à drussellx d'envoyer un message privé à DataBreaches via BreachForums pour confirmer son implication. drussellx a ensuite envoyé à DataBreaches un message privé indiquant que YuroSh était responsable du piratage.

Quel est donc le détail des rapports des médias que YuroSh souhaitait clarifier ? Eh bien, selon YuroSh,les données n'ont jamais été vendues aux enchères ou vendues tout court - et elles n'allaient pas être vendues.

Apparemment, YuroSh et drussellx avaient des priorités différentes quant à l'usage qu'ils feraient des données, mais aucun d'entre eux ne voulait vraiment vendre les données des gens ou les divulguer. Drussellx aurait voulu extorquer FREE et aurait utilisé l'annonce de la mise aux enchères et l'annonce de la vente pour essayer de faire pression sur Free afin qu'il paie l'extorsion. YuroSh, quant à lui, semblait plus motivé par l'hacktivisme, déclarant à DataBreaches :

« Chaque citoyen français a probablement été victime d'une fuite au moins une fois. Parmi les bases de données récemment piratées figurent Free, SFR, France Travail, Ameli, la CAF (Caisse d'allocations familiales), la FFF (Fédération Française de Football), Ledger, LDLC, Shadow et Cdiscount. Je ne suis pas un saint, mais j'espère que l'incident free.fr réveillera enfin les Français sur la réalité de la surveillance de masse et qu'ils lutteront contre elle. La protection de la vie privée en France a été érodée à un point tel qu'elle est pratiquement inexistante. Cette situation va au-delà d'une simple violation, il s'agit d'un problème systémique, enraciné dans un gouvernement déterminé à imposer un État de surveillance. La majorité des gens ne réfléchissent pas aux pratiques de surveillance, alors même que les GAFAM et le gouvernement s'entendent pour contrôler tous les aspects de nos vies numériques.

« La France est devenue le premier pays d'Europe à légaliser la surveillance biométrique, soi-disant pour la "sécurité publique" lors d'événements majeurs comme les Jeux olympiques. En vertu de cette nouvelle loi, la police utilise la vidéosurveillance algorithmique pour analyser les données biométriques : formes du corps, gestes, mouvements. Ils ont fait passer cette loi pendant une période de distraction nationale, balayant d'un revers de main les débats sur les libertés civiles. Il s'agit d'une décision calculée qui révèle le peu de respect qu'ils accordent à la vie privée. Cette décision ouvre manifestement la voie à une nouvelle expansion. Il ne s'agit pas de sécurité publique, mais de normalisation progressive de la surveillance de masse.

« Les forces de l'ordre françaises sont allées jusqu'à cibler ProtonMail, Tor et d'autres outils de protection de la vie privée, en les qualifiant de criminels. Elles ont rendu l'utilisation de ces protections suspecte, tout en

« Les forces de l'ordre françaises sont allées jusqu'à cibler Protonmail, Tor et d'autres outils de protection de la vie privée, en les qualifiant de criminels. Elles ont rendu l'utilisation de ces protections suspecte, tout en négligeant les violations réelles. Ils prétendent qu'il s'agit de lutter contre les cybermenaces, mais en réalité, il s'agit d'une attaque contre les libertés individuelles.

« Leur objectif est le contrôle total, et ils ne le cachent pas. Des drones de surveillance des manifestations aux systèmes de notation de l'IA qui réduisent les droits sociaux sur la base d'algorithmes mystérieux, chaque nouvel outil rapproche la France d'un État de surveillance. La vie privée est sous assistance respiratoire, et si les gens ne résistent pas maintenant, elle pourrait bientôt disparaître complètement ».

Et YuroSh d'ajouter : « Je suis différent, je déteste la surveillance et je pense que la seule façon de les réveiller est de les pirater. Sinon, les choses ne changeront pas. »

Problèmes de sécurité passés de FREE

YuroSh a précisé avec exploité une vulnérabilité dans une API. Il a concédé que « Free a une sécurité tout à fait convenable pour qui ne creuse pas trop, mais ils sont lents à répondre ». Pour lui, la multiplication des dispositifs de surveillance et des bases de données associées ne fait qu'augmenter le risque de brèches. Aussi, il « recommande que les entreprises conduisent des audits de sécurité et des recherches de vulnérabilités, réguliers, pour identifier les faiblesses dans leurs systèmes, si elles veulent vraiment savoir ce qui se passe ».

YuroSh dit enfin parfois conserver les données piratées, parfois les supprimer. Dans le cas de celles de Free : « je ne sais pas encore ».

YuroSh a également affirmé que dans le passé, ils avaient envoyé à FREE des alertes de vulnérabilité qui ont été ignorées. En fait, FREE a déjà été condamné à une amende par la CNIL dans le passé. Le 30 novembre 2022, la CNIL a infligé une sanction de 300 000 euros à FREE, pour non-respect des droits des personnes et de la sécurité des données de ses utilisateurs.

Selon l'annonce de la CNIL, une enquête de la CNIL en réponse à des plaintes de consommateurs avait révélé plusieurs violations du RGPD, notamment des mots de passe en clair, et la remise en circulation d'environ 4 100 Freebox mal reconditionnées.

DataBreaches a demandé à YuroSh si les vulnérabilités qu'ils avaient signalées à FREE l'avaient été avant ou après novembre 2022. Il a répondu que c'était après cette date, et facilement « parce qu'ils n'ont pas bien surveillé, nous avons pu envoyer des millions de requêtes pendant des semaines ».

La CNIL a annoncé la mise en place d'un formulaire pour porter plainte... puis s'est rétractée

Dans la foulée, la Commission nationale de l'Informatique et des Libertés avait annoncé la mise en place d'un formulaire en ligne : « si vous avez été avisés de la violation de vos données, à la suite de la cyberattaque visant l'opérateur de téléphonie Free, vous avez la possibilité de porter plainte via un formulaire en ligne sans vous déplacer en commissariat ou en brigade de gendarmerie. Ce formulaire sera prochainement disponible depuis le site cybermalveillance.gouv.fr ».

À la surprise générale, la mention du formulaire en ligne, sur la page consacrée au piratage de Free de la CNIL, a finalement disparu, sans qu'aucun formulaire ne soit mis en ligne. La Commission a confirmé que le formulaire en ligne « n'était plus d'actualité depuis la semaine dernière » sans pour autant apporter d'explications permettant d'en comprendre la raison.

Sources : CNIL (1, 2), DataBreaches

Et vous ?

➡ Quel rôle les entreprises comme Free devraient-elles jouer pour prévenir les cyberattaques ? Les mesures actuelles de sécurité dans le secteur des télécoms sont-elles suffisantes pour rassurer les consommateurs ?
➡ La communication de crise de Free est-elle appropriée selon vous ?
➡ Le piratage des IBAN et données sensibles doit-il entraîner des compensations pour les clients ? Les entreprises doivent-elles prévoir des mécanismes de soutien financier pour leurs abonnés en cas de vol de données sensibles ?
➡ Comment les utilisateurs peuvent-ils mieux protéger leurs données personnelles ? Les consommateurs devraient-ils être davantage sensibilisés et formés aux risques de cybercriminalité ?
➡ Le déploiement d'un formulaire de plainte en ligne est-il suffisant en cas de piratage de grande ampleur ? Les consommateurs ont-ils accès à des moyens de recours appropriés dans de tels cas ?

Voir aussi :

➡ Free : les données personnelles de 14 millions de clients en vente sur le dark Web. Faux, affirme Free

0 COMMENTAIRE

Commenter Signaler un problème